

PATENT

Attorney Docket No. 26796.2

**CENTRALIZED AUTHORIZATION AND FRAUD-PREVENTION
SYSTEM FOR NETWORK-BASED TRANSACTIONS**

Inventor: David P. Cook
Dallas, TX
citizen of U.S.

Assignee: ZixIt Corporation
13355 Noel Rd., Suite 1555
Dallas, Texas 75240

HAYNES AND BOONE, L.L.P.
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
(214) 651-5000

054207-8962460

EXPRESS MAIL NO. <u>EJ 856342731 US</u>	DATE OF DEPOSIT <u>10/27/99</u>
This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231	
<u>KAREN A. HARRIS</u> Name of person mailing paper and fee	<u>Karen A. Harris</u> Signature of person mailing paper and fee

CENTRALIZED AUTHORIZATION AND FRAUD-PREVENTION SYSTEM FOR NETWORK-BASED TRANSACTIONS

TECHNICAL FIELD

This invention relates generally to electronic commerce and, more particularly, to a system and method for authorizing certain aspects of network based transactions.

BACKGROUND

There are many emerging trends in the communications world, including the increase in network technology and the proliferation of data networks. These trends have advanced the proliferation of e-commerce, i.e., commerce that occurs over an electronic network such as the Internet. E-commerce enables certain customers to purchase goods and services using an account number by contacting a merchant directly over the network. Common e-commerce scenarios include a person at home using a credit card to purchase a product from an on-line store over the Internet, and an employee of a corporation acting as a buyer/authorizer for acquiring resources using a company issued account number.

One difficulty commonly addressed in e-commerce transactions is that, because of potential theft or fraud, customers are reluctant to provide personal and/or confidential information over the network. One common response is to utilize secure network transmissions by using technologies such as Secure
5 Sockets Layer (SSL) or Secure HyperText Transmission Protocol (HTTPS). However, this response is only a partial solution because many customers, although willing to provide some confidential information such as an account number, may still not be willing to provide other confidential information such as a Personal Identification Number (PIN) or other account code. One reason
10 for such reluctance is because the customer would be extremely vulnerable if both the account number and PIN were stolen. As a result, PINs have not heretofore been successfully adopted and used in e-commerce transactions.

PIN and other account code authorization systems are used, however, in many face-to-face transactions, such as at a grocery store. Face-to-face
15 transactions are inherently less susceptible to theft or fraud, making these account code authorization systems less necessary. E-commerce remains more susceptible to theft or fraud than most face-to-face transactions.

The reluctance of the customer to provide a PIN or other type of account code over a network also differentiates e-commerce from other non-
20 face-to-face transactions, such as automated teller machines. With automated teller machines, PINs are typically required, along with a physical credit card, to access a specific account, thereby providing an additional element of security. Automated teller machines, in general, provide customers with sufficient security (actual or perceived) to overcome their reluctance to provide
25 their PIN.

Another difference between e-commerce and face-to-face transactions is that a customer cannot physically "sign" a completed sales event. For

example, in face-to-face transactions, a customer is typically given an authorization form such as a paper charge slip, with a final charge amount printed thereon. The customer then physically signs a name on the slip, thereby authorizing the transaction. However, equivalent "signing" procedures for e-commerce transactions are not currently generally available.

For these and other reasons, it is common that account issuers and/or conventional authorization and fraud detection systems will not guarantee payment for e-commerce transactions. As a result, the merchant is often left with the financial loss that occurs when an account number has been fraudulently used in the transaction. Furthermore, some customers are less likely to utilize e-commerce because of a perceived security inadequacy.

What is needed is a system and method that helps to prevent, reduce, and/or eliminate fraudulent acquisition of customer account information used for e-commerce transactions.

Furthermore, what is needed is a system and method that helps to authorize customer account information and prevent fraudulent use of customer account information.

Further still, what is needed is a system and method that allows the merchant to authorize an e-commerce transaction in a relatively simple manner.

Further, what is needed is a system and method that is relatively easy to implement by both the customer and the merchant, and that does not require an excessive amount of keystrokes or actions for any single transaction.

SUMMARY

In response to these and other problems, provided is a new and unique system and method for authorizing certain aspects of network based transactions between a customer and a merchant. In one embodiment, the system includes means for identifying rights (such as ownership) to use an account identified by an account number, and a database for storing the account number and a Signature Phrase. The Signature Phrase is stored when rights to use the account have been positively identified. In some embodiments, the means for identifying rights to use the account utilizes an account code. In other embodiments, the means for identifying rights to use the account may access an account issuer or other third party. The account code may be received through an external interface with the customer. In some embodiments, the database stores the account number and the Signature Phrase in a transformed format.

The system also provides a second interface for receiving an account number and Signature Phrase from the customer for comparison with the account number and Signature Phrase stored in the database. In some embodiments, either interface may be through a network and the second interface may include a network-based authorization form. The authorization form may include many custom features, such as a greeting phrase previously provided by the customer to the database and/or a logo identifying the merchant. In some embodiments, the second interface may also receive the account number and the Signature Phrase in a transformed format.

The system also includes a comparator for comparing the account number and Signature Phrase stored in the database with the account number and Signature Phrase received from the customer during the transaction. The

comparator may simply be a set of software instructions running on a computer. If the comparison succeeds, the system authorizes the transaction.

The system may also provide a transaction certificate to memorialize a successful authorization. The transaction certificate may be provided to the merchant or elsewhere.

In another embodiment, the system includes a computer engine and a database having a list of linked account numbers and Signature Phrases. The computer engine receives authorization requests from the merchant and processes the requests by verifying rights in the account with the customer-provided Signature Phrase. If verified, the system returns a transaction certificate to the merchant.

The present invention also provides a method for authorizing an e-commerce transaction. The method confirms rights in the account by associating an account code with an account number assigned to the account. If the rights are confirmed, a Signature Phrase is established and linked to the account number. Rights to the account, such as those normally only associated with the account code, can then be extended to the customer, thereby authorizing the transaction made on the account using the Signature Phrase.

An entity other than the customer may also confirm the rights in the account. For example, if the account is shared by members of a family, one member can confirm the rights in the account and then another member can establish and use the Signature Phrase for the transaction. In another example, if the account is shared in a corporation, the corporation may confirm the rights and an employee can use the Signature Phrase for the transaction.

In another embodiment, the method links the account code to the account number to enable the customer to confirm rights to the account. When the rights to the account are confirmed, the customer may create a

Signature Phrase linked to the account number. Thereafter, a transaction authorization request for the account can be authorized by linking the Signature Phrase to the account number.

BRIEF DESCRIPTION OF THE DRAWINGS

5 Fig. 1 is a diagram of a network and several nodes for implementing one embodiment of the present invention. The nodes represent a customer, a merchant, and an authorization system.

 Fig. 2 is an illustration of a portion of a database in the authorization system of Fig. 1.

10 Fig. 3 is an illustration of a screen for activating or modifying an entry in the database of Fig. 2.

 Fig. 4 is a flowchart of an account activation/modification process.

 Fig. 5 is a flow chart of a transaction process.

15 Fig. 6 is an illustration of a screen of an exemplary transaction being performed by the process in Fig. 5.

 Fig. 7 is a flow chart of an authorization process.

 Fig. 8 is an illustration of a screen of an exemplary authorization being performed by the process of Fig. 7.

DETAILED DESCRIPTION

5 The present invention provides a unique system and method for authorizing certain aspects of network based transactions. It is understood that the following disclosure provides many different embodiments, or examples, for implementing different features. Techniques and requirements that are only specific to certain embodiments should not be imported into other embodiments. Also, specific examples of networks, components, and formats are described below to simplify the present disclosure. These are, of course, merely examples and are not intended to limit the invention from that described in the claims.

10 A number of items are used herein to describe certain account information.

15 "Account number" refers to a number that identifies a specific account from an account issuer. One example of an account number is a credit card number issued from a bank or other financial entity. Another example is a corporate charge account number provided by a corporation. Additional examples of account numbers include debit card numbers, organizational card numbers, membership identification numbers, social security numbers, e-mail addresses, and the like.

20 "Account code" refers to a unique number or phrase that is assigned to a specific account by the account issuer and indicates certain rights, such as ownership, to the account. Often, the account code is used to verify that the user of a specific account number is legitimate. Common examples of account codes include PINs, employee codes, and passphrases.

25 "Signature Phrase" is a term used in the following disclosure to indicate a new and unique phrase associated with a particular account and that is

created either by the user/owner of the account or by the account issuer. The Signature Phrase is not associated with the account, except as provided in the present disclosure. There may be multiple Signature Phrases for a specific account.

5 “Activation code” is a term used in the following disclosure to designate numbers or phrases that are used to access, activate, or modify a database entry of the present invention that relates to a specific account. An activation code may be an account code or a Signature Phrase.

Exemplary Network

10 Referring now to Fig. 1 of the drawings, the reference numeral 10 designates, in general, a system for implementing electronic commerce (e-commerce). The system 10 is centered around a network 12, which may be any combination of the Internet, local area networks, and Intranets. For the sake of example, the network 12 will be considered to be the Internet and will
15 utilize Transfer Control Protocol/ Internet Protocol (TCP/IP) to transmit data between various nodes connected to the network. Communication techniques such as Secure Sockets Layer (SSL) or Secure HyperText Transmission Protocol (HTTPS) can be used to provide extra security for Internet transactions.

20 Three nodes 14, 16, and 18 are illustrated as being attached to the network 12. The nodes 14-18 are illustrated as personal computers, but it is understood that each node can actually represent one or more different computing devices, including mainframes, servers, wireless telephones, personal digital assistants, and the like.

25 Referring to node 14 for example, the node includes a processing unit, a memory, and a network interface, generally represented as computer 14a. The

computer 14a also includes a customer interface, which in the present example includes a monitor 14b and keyboard 14c. It is understood that each of the listed components may actually represent several different components. For example, the computer 14a may actually represent a distributed processing system including different levels of main memory, hard disks, server/client memory, and remote storage locations. Furthermore, it is understood that, in many implementations, the nodes 14, 16, and 18 may be configured differently from each other and/or may have different components.

In continuance with the present example, the node 14 will represent an e-commerce customer who wishes to purchase an item or to otherwise authorize a transaction, and the node 16 will represent an e-commerce merchant willing to sell the item or complete the transaction. The node 18 will represent an authorization system that will facilitate the transaction between the customer 14 and the merchant 16.

In the present embodiment, before the transaction is completed, two preliminary steps may be performed pertaining to the authorization system 18. First, a database 50 of various entries is established. The entries correspond to account numbers and other related information. In one example, account numbers and other related information are furnished by account issuers to the authorization system. In another example, an account number and other related information may be provided by the customer, either before initiating a transaction or during the transaction.

Second, a particular entry in the database 50 must be activated. Once activated, a person or other entity having rights to an account identified by the account number can authorize e-commerce transactions using a Signature Phrase. If the entry is self-activating, as discussed further below, this second step may not be necessary.

Once these steps have been performed, the customer 14 can complete an e-commerce transaction using the customer's account by providing a Signature Phrase without the Signature Phrase or account code actually residing at the authorization system 18 or being provided to the merchant 16. The completion of the transaction may also include a certification process for further authentication. Both the transaction completion and the certification process are individually discussed in greater detail below. It is understood, however, that different embodiments may utilize some steps while not utilizing others. Furthermore, a wide range of modifications, changes and substitutions are intended in the following disclosure.

The Database

Referring also to Fig. 2, in one embodiment, the authorization system 18 includes a database 50 having one or more entries, represented by entries E1 and E2. Each entry may include one or more records, and each record may include one or more items. It is understood that the illustration of the database 50 in Fig. 2 is not to scale, and the illustrated size of specific entries, records, and items is not indicative of the actual size of each.

In furtherance of the present example, entry E1 includes four records: a header record 52 and three H3 records 54, 56, and 58. These records are filled with various items at different times, and may be expanded or compressed as necessary.

The header record

The header record 52 includes an account identifier 60 that identifies a unique account number for a specific account. In the present example, the account identifier 60 includes two items: H1 and H2. The H1 item represents

the result of a hash function on a particular account number for the customer 14 (Fig. 1), as represented by the following formula:

$$H1 = \text{Hash}(\text{account number}) \quad (1)$$

A hash function is an example of a data transformation function that is performed on a string of data (the account number in the present example) to generate a unique representation (the "hash") corresponding to the string of data. The hash is generated in such a way that it is extremely unlikely that some other text will produce the same hash value. In one implementation, a message digest five (MD5) hash function is applied to the account number to produce a 128-bit representation of that number. It is also understood that the hash is a one-way function. That is, the account number cannot be derived from its hash.

The H2 item represents the hash of the account number combined with a bit string, denoted P1, as represented by the following formula:

$$H2 = \text{Hash}(\text{account number} + P1) \quad (2)$$

The bit string P1 may be a published, widely known constant. By having the extra item H2, two hashes representing the account number are created, thereby further securing a unique identity for each particular entry in the database 50. By using both items H1 and H2, it is possible to identify the entry E1 for one and only one account number. Also, it is understood that in the present example, the actual account number is not stored in the database 50. Instead, only the items H1 and H2 are stored. Since each account number produces a unique hash pair, the account number is, in effect, stored in the database 50 by the reference to the two hashes. Furthermore, since the account number cannot be derived from the hashes, the account number cannot be obtained by computer hackers or other personnel.

The header record 52 also includes a SIGPHRASE item that stores the Signature Phrase to be used with, or instead of, the account code previously assigned to the account. For example, since a customer may be reluctant to use a bank-issued PIN in e-commerce transactions, the customer can establish the Signature Phrase to act in lieu of the PIN. As a result, the Signature Phrase works identically to the PIN in e-commerce transactions, but does not work in other transactions such as automated teller machines. The Signature Phrase may be a relatively long alphanumeric string, the extended length of which increases overall security. This item is preferably hashed for security reasons.

Each entry in the database 50 may also include one or more additional items. Certain items may be associated with the header record 52 while other items may be associated with one or more H3 records 54-58. The number and arrangement of items in any particular record is flexible to specific applications and/or preferences. These additional items are collectively illustrated as an OTHER item in the database 50, and may include one, more, or all of the items listed in Table 1, below.

Item	Description
ISSID	Identifies the account issuer
LOGO	Identifies entity associated with the account
NOTE	Options for issuer notifications of authorizations
POLICY#	Issuer policy parameter sheet to be applied to this entry
EMAILID	E-mail address of customer or appropriate entity
EMAILOP	E-mail rules
EDITID	Master editing code
CSTAT	Card or account status

Item	Description
FSIG	Forced signature
DATES	Dates record was created or updated
STATUS	Current status of record
GP	Greeting phrase for authorization form
2ndPH	Additional Signature Phrase with restrictions
2ndPH\$	Restrictions for the Signature Phrase 3rdPH
3rdPH	Additional Signature Phrase with restrictions
3rdPH\$	Restrictions for the Signature Phrase 3rdPH

Table 1

It is understood that all of the items in Table 1 are merely illustrative. Many different items can be used instead of, or in addition to, any of the items herein discussed. Several of these items are provided when the entry is created, either by the issuer or by a specific customer (certain entries can accommodate multiple customers, each with a unique Signature Phrase). Other items may be modified, accessed, or removed at various times, such as is discussed in the "Account Activation and Modification" section, below.

The ISSID item identifies the account issuer. The issuer may be a particular bank or other financial entity, a corporation that has provided purchasing accounts to its employees to allow the employee to incur indebtedness on its behalf, or other similar entity. In the corporation example, the issuer may designate the corporation itself or a specific department in the corporation. In some embodiments, the customer cannot alter this item.

The LOGO item provides a logo that can represent various entities, programs, or the like that are associated with the account number. For example, the LOGO item may identify a particular airline whose logo appears

on a credit card associated with the account number. Alternatively, or in addition, the LOGO item may represent a card member status, such as a "gold" or "platinum" member. Further still, the LOGO item may include a Graphics Interchange Format (GIF) sub-item that can be used for visual enhancement. In some embodiments, the customer cannot alter this item.

The NOTE item allows the account issuer to provide specific notifications for authorizations by this account. For example, a corporation may provide purchasing accounts to various employees, yet still desire to exercise a certain amount of control over the account. This NOTE item may indicate, for example, that a notification of all transaction authorizations by this account should be sent to the corporate accounting department. The NOTE item may also be customer-specific, such as allowing the president of the corporation to conduct transactions without notifying the accounting department. Further still, the NOTE item may include an e-mail address sub-item to which notifications may be sent. In some embodiments, the customer cannot alter this item.

The POLICY# item is a reference number to a parameter sheet associated with the particular entry. The parameter sheet may have general formatting and rules that can be applied to the authentication and transaction processes. For example, a corporation can assign a specific class identifier to the customer/employee 14. Employees in class "A" may have one specific group of restrictions, and employees in class "B" may have a different group of restrictions. In some embodiments, this item cannot be later altered by the customer/employee.

The EMAILID item is an e-mail address for communication to the customer 14 or other desired recipients. The e-mail address may be used, for example, when it appears someone other than the customer is attempting to

use the customer's account number in a transaction. The authorization system 18 can send an e-mail to the designated recipients informing them of each account usage or only that the account is apparently being improperly used. Another example use of the e-mail address is if a customer with specific restrictions attempts a transaction that contradicts those restrictions, the authorization system 18 can send an e-mail notifying the account issuer of the transaction. In some embodiments, the customer cannot alter this item.

The EMAILOP item is a set of rules to specify when e-mail notification is to occur. For example, certain customers may request notification upon every transaction, every transaction that fails authorization, or every transaction over a certain dollar amount. In some embodiments, the customer cannot alter this item.

The EDITID item is a master-control item that allows the issuer to make changes to the entry. This item may act as an issuer-version password code that allows the issuer to make edits to the entry. For example, a corporation may cancel an account of an employee who is leaving the company. This item is preferably hashed for security reasons. In some embodiments, the customer cannot alter this item.

The GP item is a greeting phrase that is selected by the customer in the activation process and can be used during transaction authorization. For example, the greeting phrase may be "Hello Ms. Smith", or may preferably be a more personalized quote, such as "How about those Dallas Cowboys!" The greeting not only personalizes the transaction, but also serves as a subtle identifier for the authorization system 18. That is, the customer 14 can distinguish the authorization system 18 from other systems that do not have the greeting phrase, as will be discussed in greater detail in the Transaction section below.

The 2ndPH and 3rdPH items are additional, specialized Signature Phrases. These additional Signature Phrases can identify certain transaction restrictions. An example is if the customer establishes a separate Signature Phrase for a child. The child may use the account according to the restrictions. These items are preferably hashed for security reasons. In some embodiments, the customer cannot alter this item.

The 2ndPH\$ and 3rdPH\$ items are lists of restrictions for a particular customer who uses an additional specialized Signature Phrase 2ndPH and 3rdPH, respectively. One example of a restriction is a money limit per transaction. In some embodiments, the customer cannot alter this item.

The CSTAT item may include generic account status descriptions, such as "live," "dead," or "suspended." In some embodiments, the customer cannot alter this item.

The FSIG item is used for a corporate issuer to mandate a particular Signature Phrase to be used for the account. That is, the corporate issuer does not want the customer/employee to change the Signature Phrase. In some embodiments, the customer cannot alter this item.

The H3 record

Each of the H3 records 54, 56, and 58 includes a representation of an account code for the account identifier 60 in question. In the case of credit card issuers, the account code may be a PIN. In the case of corporate account issuers, the account code may be an employee code. As will be discussed in greater detail below, the account code can be used as an activation code for initial account activation and accessing the account thereafter.

In the present example, the account code is represented by an item H3, which represents the hash of item H1 combined with the account code, as represented by the following formula:

$$H3 = \text{Hash}(H1 + \text{account code}) \quad (3)$$

5 By storing the hash of the account code in the H3 record, instead of the actual account code, an additional level of security is provided.

Each of the H3 records 54, 56, and 58 may be formatted in different ways, and may have different data stored therein. The actual number of H3 records is also flexible. For example, there may be no H3 records at all, or
10 there may be many different H3 records. Data management routines can be used to maintain the number of H3 records to an appropriate amount. In the present embodiment, if there are no H3 records, then some item must eventually be provided to verify a specific customer's use or access to the entry. For example, a corporation may utilize the FSIG item to mandate a particular
15 Signature Phrase to be used for the account entry. In this example, there is no H3 record, only a Signature Phrase and other header record items.

Each H3 record may also include a DATE item and a STATUS item. The DATE item represents the time when the record was entered in the database 50. In some embodiments, this item is automatically updated.

20 The STATUS item identifies a current status of the respective record. In some embodiments, this item can be altered by the customer or the account issuer. For the sake of example, Table 2 below illustrates possible STATUS values.

Value	Description
1	The H3 record was used in an account activation or modification process.
2	The H3 record has not been used in an account activation or modification process.

Table 2

5 The specific use of the DATE and STATUS items is discussed in greater detail in the "Activation and Modification" section and the "Transaction" section, below.

Database population

10 The database 50 can be populated with entries in various ways. One way is for the database to receive data from one or more account issuers (e.g., banks or corporations). The data may be delivered electronically or may be manually entered, such as through one or more data storage or transmission mediums. The minimum amount of information required to initially populate the database is the account number.

15 The account issuer, generally, delivers the account number (or hashes H1 and H2) and the account code (or hash H3) to authorization system 18. If the actual account number and/or account code(s) are delivered (preferably by secure means), the authorization system can, in one embodiment, format the data appropriately and perform the hash functions and store the hash values
20 for H1, H2, and H3 in the database. If hash values H1, H2, and H3 are provided by the account issuer, they are stored in the database. Once hash values H1, H2, H3 have been generated and stored, the actual account number and/or account code(s) can be erased. Alternatively, the database could store the actual account number and account code, which would become items H1,

H2, and H3 in the database. While this latter embodiment is less secure, it may be easier for the issuer, merchant or customer to implement.

In another embodiment, as discussed in the next section, the customer manually provides the account number, account code, and the Signature
5 Phrase to the database 50 at the time the customer creates/activates the account.

Account Activation and Modification

Once the database 50 has been established, but before the authorization
10 system 18 can be used to complete an actual transaction (discussed in greater detail below), the specific entries of the database involved in the transaction should be activated.

There are various methods for activating the entries in the database 50. For one, the entries may be self-activated. That is, once the data for the entry is provided to the authorization system 18, transactions may use the entries
15 accordingly. For example, a corporation may provide an employee with an account number and a Signature Phrase that is already activated (FSIG, Table 1).

The activation and modification process may be performed by the customer 14 separately from any transaction, or may be initiated during a
20 specific transaction. These and other methods are discussed in greater detail with reference to Figs. 3 and 4

Referring to Fig. 3, in one embodiment, the customer 14 may initiate an activation and modification process by accessing a specific site 80 on the
25 network 12. In the present example, the network 12 is the Internet and the specific site is a site that is provided by, or associated with, the authorization system 18. For the sake of clarity, the site 80 is illustrated as a screen in Fig.

3, such as may appear in a web browser on the customer's computer 14a. In actuality, the site 80 is a set of computer instructions that reside on a server connected to the network, such as the authorization system 18. In addition to the screen, the site 80 may also include various functional routines that may or may not be apparent to the customer 14. Some of these functional routines may be provided to and reside on the customer's computer 14a, while other functional routines may reside on the computer that is supporting the site 80 (e.g. the authorization system 18).

The site 80 may be accessed, for example, by the customer 14 entering a Uniform Resource Locator (URL) on the customer's computer 14a. The URL may be provided to the customer 14 in various manners. For example, the issuer of the account may mail the URL to the customer along with the account code. Alternatively, the URL can be provided by the merchant 16, can be linked from the account issuer's own web site, or other possible methods. Upon accessing the site, a screen 81 will appear on the monitor 14b of the customer's computer 14a.

In the present example, the screen 81 includes a logo 82. The logo may be specific to the authorization system 18, or may instead be specific to the issuer of the account number being activated. Although optional, the logo 82 can provide a certain degree of comfort to the customer 14 that the site is authentic, thereby encouraging the customer to complete an activation and modification process.

The screen 81 also includes instructions 84 and inputs 86 and 88 to receive the customer's account number and activation code (account code (e.g., PIN) or Signature Phrase). Although the illustrated instructions 84 are quite simple, they may be more elaborate to provide more information about the activation and modification process.

In some embodiments, the site 80 includes one or more scripts 90 running in the background of the customer's computer 14a. The scripts 90 are illustrated in phantom because, although they reside on the customer's computer 14a, they may not be visible on the monitor 14b. For example, the scripts 90 may include the hash function (as used equations 1, 2, and 3, above) and other necessary instructions. Once the account number and account code or Signature Phrase have been entered into the inputs 86, 88, the customer may then select the "Access or Activate Account" option 92 to initiate an activation and modification process.

Referring now to Fig. 4, one embodiment of an activation and modification process is designated generally with the reference numeral 100. The activation and modification process 100 is not only used for activating an entry in the database 50, but may also be used to enter, access, or change certain items in a specific database entry.

Execution of the activation and modification process is initiated at step 102 by the customer 14 accessing the authorization system 18. In the present example, the customer 14 accesses the authorization system 18 by entering the account number and an activation code for inputs 86, 88 and selecting the Access or Activate Account option 92, as discussed above with reference to Fig. 3.

At step 104, a hash is created for the account number. In the preferred embodiment, the hash is created at authorization system 18. In another embodiment, the hash is created at the customer computer 14a. At step 106, the H1, H2 values are compared to H1, H2 items in the database 50 (Fig. 2) and at step 108, a determination is made as to whether the H1, H2 values derived from the account number provided by the customer 14 are in the database 50.

If the hash values H1, H2 are in the database 50, a specific entry is identified and the authorization system 18 may now erase the actual account number (if any was provided). By erasing the actual account number as soon as possible, the possibility of theft is reduced. Execution then proceeds to step 110, where the authorization system 18 hashes the entered activation code (account code or Signature Phrase) and compares the hash value to the signature phrases (e.g., SIGPHRASE, 2ndPH, 3rdPH) in the account. Should this compare fail, the hash value is compared to the latest H3 record for the account. If at step 111 either compare succeeds, the account may be made available for viewing or update purposes.

Execution then proceeds to step 114 where the authorization system 18 determines if the customer 14 may enter, access, or change items in the account entry. If the customer 14 is allowed to access or change specific items in the entry, execution proceeds to step 116 where the customer may change the specific items (such as in Tables 1 and 2, above) accordingly. An example of one change is activating the account entry if not already activated. The customer 14 may be prompted to provide a Signature Phrase, which is stored in the SIGPHRASE item in the header record 52, if one has not yet been provided. In another embodiment, the account issuer (such as a corporation) may have already provided a forced Signature Phrase (e.g., using the FSIG item in Table 1). Other items may also be accessed, updated, or changed, as allowed by any previous restrictions to the account entry.

As discussed below under "Transaction," the Signature Phrase will act as an authorizing code in the e-commerce transaction. The extended length of the Signature Phrase increases overall security. In the preferred embodiment, a hash of the Signature Phrase is stored in database 50. In the present

example, the account number and the Signature Phrase are now activated for transactions.

If the activation code provided by the customer 14 is not found in the specified entry at step 111, then execution proceeds to an error handling routine at step 118. In one implementation, the error handling routine 118 initiates an additional attempt at authorization by using external systems, such as an automated teller machine network. The appropriate entity (e.g., the customer 14) may also be informed of the current situation, be it by error (e.g., the customer typed in the wrong activation code) or other condition. Alternatively, the error handling routine 118 may simply provide a message to the customer 14 to help the customer provide a proper activation code and return execution to step 110. In one implementation, the customer 14 is allowed only two attempts at providing a proper activation code. If two successive attempts fail, the account entry will be locked from further activity for an extended period of time. This effectively eliminates "brute-force" attacks on the activation code.

If an account issuer has not previously populated the database with the account number, then at step 108 the hash values H1, H2 would not be in the database 50. Then, execution would proceed to step 120, where the account number and account code (if necessary) are submitted by authorization system 18 for a separate (and normally external) authorization process. For example, the separate authorization process can be a standard authorization technique of account numbers and account codes, such as is used by automated teller machines for PIN verification. Other separate authorization processes may not require an account code. At step 122, in this example, a determination is made as to whether the separate authorization process indicates a valid account number and account code (if necessary). The customer 14 may be

662007-8962460

5 further prompted to update additional needed items for verification, such as a credit card expiration date. If the separate authorization process did indicate a valid account number and account code (if necessary), execution proceeds to step 124 where a new database entry including H1, H2, and H3 (if applicable) is created. Execution then proceeds to steps 114 and 116 described above. At step 116, the customer is prompted to provide a Signature Phrase, which is stored under SIGPHRASE in the header record 52.

10 Alternatively, the authorization and modification process 100 can provide the account number to a third party (e.g. the account issuer) at step 120, who may authorize the activation of the account. If the account is authorized at step 122, then at step 124 the third party may provide a Signature Phrase for use by the customer 14. The Signature Phrase may be a forced signature, such as is indicated by the FSIG item in the header record of the newly created account entry.

15 If at step 122 the separate authorization process or third party did not indicate a valid account number and activation code or did not otherwise authorize the account, execution proceeds to the error handling routine 118.

20 In some embodiments, activation may be an automatic update that occurs immediately upon a match between the activation code and the H3 record or previously stored Signature Phrase (step 111) or upon successful authorization (step 122). For example, once the customer enters the proper account number and account code, the STATUS value for the H3 record of the identified account code, if available, is now set equal to 1 (Table 2). Additionally, the CSTAT value may be set to an active status.

25 Not only does the activation and modification process 100 allow the customer 14 to activate a pre-existing entry in the database 50, it also allows the customer to access, enter, or change certain items in the entry. In some

embodiments, an account entry that is not activated is only accessed with an account code. Once the account is activated, the account entry may be accessed with an account code or a previously created Signature Phrase. The Signature Phrase works similarly to the account code, with any restrictions and permissions that are dictated by the items in the identified account entry.

Referring again to steps 110-114, in some embodiments, a specific account entry may have several Signature Phrases, and permission to enter, access, or change certain items may be different for each subordinate Signature Phrase of the account. For example, a family of customers may have a single account number with different Signature Phrases for different members of the family. Depending on the Signature Phrase provided to access the account entry, certain items may or may not be accessible for review, change, update, and/or deletion. Furthermore, in one embodiment, if the account code, rather than the Signature Phrase, is used to access the account, the customer will not be permitted to view previously established database information, but will be permitted only to create new information. This would prevent an unauthorized person that has obtained a customer's account number and account code from viewing all of the customer's previously established account information.

The Transaction

Just as there are many different types of customers 14, networks 12, and merchants 16, there are also many different transaction scenarios. Referring to Fig. 5, a general transaction method 150 is disclosed, it being understood that the general transaction method 150 is directed to just one example scenario.

At step 152, the customer 14 selects various items at one or more merchant 16 Internet sites by accessing the merchants over the network 12. At step 154, the customer 14 goes to checkout at the merchant site and fills in the necessary information and at step 155, then customer 14 initiates authorization. At step 156, the merchant 16 prepares and forwards specific information to an authorization process. In one implementation, the specific information is forwarded as "BUY" button 212 (Fig. 6) in HTML format.

Referring also to Fig. 6, for the sake of example, the merchant 16 is an Internet bookstore and the customer 14 selects two books using an Internet browser connected to the bookstore's web site. An exemplary screen 200 of the bookstore's web site includes a logo 202 for the merchant, a description of the items being purchased 204, credit card account information 206, a shipping address 210, and a BUY button 212. In accordance with step 154 (Fig. 5), the customer 14 has filled in the necessary information, which in the present example includes credit card information including card number and a shipping address. The customer 14 has also initiated an authorization process by selecting the BUY button 212 using an appropriate key on the keyboard 14c (Fig. 1).

In the present example, the BUY button 212 is specifically associated with the authorization system 18. The BUY button 212 includes several functional items provided by the merchant, such as one or more of the items listed in Table 4, below.

Item	Description
TURL	Target link (URL) to a specific site on the authorization system 18
CC#	Account number (e.g., credit card number).

Item	Description
RURL	Return link (URL) to screen 200 on the merchant's computer
MID	Merchant identification
AMT	Amount of the transaction
REF	A merchant's transaction reference number
TD	A description of the transaction
CUSTID	An e-mail address for the customer
MSIG	Merchant's digital signature of the present data

Table 4

The CC# item may simply be the actual account number (not preferred for security reasons), or may instead be a representation of the CC# such as with the hashes H1, H2 (equations 1 and 2, above).

The CUSTID item may be used by the authorization system 18 to communicate directly with the customer 14. For example, if the account number is not in the database 50, the authorization system 18 may send an e-mail to the customer 14 encouraging the customer to create and activate an entry for the account number.

The MSIG item represents the digital signature of the merchant and might not be used in every embodiment. Some or all of the Table 4 items in the BUY button 212 are assembled and hashed for use in creating the MSIG item. The digital signing process is described in co-pending U.S. Patent Application Ser. No. 09/340,853, filed June 28, 1999, and the contents of which are hereby incorporated by reference as if reproduced in their entirety. The resulting MSIG item authenticates the information and enables the authorization system 18 to confirm that the information has not been tampered with. Furthermore, certain items collected in Table 4 may be

encrypted using public key encryption using the public key of authorization system 18. The public key encryption process is also described in the above-referenced and presently incorporated patent application. The information is then electronically sent to the authorization system 18. On the other end, the authorization system 18 performs applicable signature verification and decryption processes, as described in the above-referenced and presently incorporated patent application

Referring now to Fig. 7, one embodiment of the authorization process is designated generally by the reference numeral 250. The authorization process may be performed at the authorization system 18 after being accessed through the Internet link indicated by the TURL included in the BUY button 212 of Fig. 6.

At step 252, the authorization process receives the information sent from the BUY button 212. The authorization process may check the received MID item (Table 4) to verify the merchant 16 may use the authorization system 18 and, further, may check the validity of the MSIG digital signature against appropriate data provided within the BUY button. In one embodiment, the BUY button 212 has the already hashed account number values H1 and H2, so the authorization process receives the account information as H1, H2. In another embodiment, the BUY button 212 has only the account number. In this embodiment, the authorization process 250 hashes the received account number. In another, less secure, implementation, the account number stored in the database 50 is not hashed. Such a determination is made responsive to the format of the items in the database 50.

At step 254, a determination is made as to whether there is an entry in the database 50 that corresponds with the received account number or hash

values. If the account number or hash values are not in the database 50, execution proceeds to step 255 and a RETURN code is returned to the merchant 16. Table 5, below, lists several potential RETURN codes.

Code	Description
1	Account number not on file.
2	Account number in database, account not activated.
3	Account number in database, Signature Phrase given is good.
4	Cancel button selected - No Signature Phrase given.
5	Account number in database, Signature Phrase given is bad.
6	Account number in database, Signature Phrase given is good, restriction violation.
7	System not available.
8	Merchant signature is bad.
9	Transaction already processed.
10	Date/Time Expired.
11	Improper merchant delivery.

Table 5

If at step 254 there is a corresponding entry, execution proceeds to step 256 where a authorization form is created for display on the customer's computer monitor 14b. The authorization form is created using data from the BUY button 212 and the corresponding account in database 50. At step 258, the authorization form and any necessary scripts (or other instructions) are provided to the customer's computer 14a.

Referring now to Fig. 8, a typical example of an authorization form is generally designated with the reference numeral 300. The authorization form 300 may utilize several of the items included in database 50. Since a wide

range of flexibility is anticipated in items overall, many different authorization forms can be created. The authorization form 300 includes a merchant logo 302 and an issuer logo 304, derived from the LOGO item in the entry in the database 50. In the present example, the merchant logo 302 is "BOOKSTORE WEBSITE" and the issuer logo 304 is "CENTRAL AIRLINES VISA."

5 The authorization form 300 also includes the custom greeting 306 derived from the GP item. The custom greeting 306 provides a level of comfort and familiarity to the customer 14, and also provides some assurance that the customer is indeed communicating with the authorization system 18. Since
10 valuable information is being considered, some entities (e.g., merchants or thieves) may try to duplicate ("spoof") the appearance of the authorization system 18 as seen by the customer 14 in performing a transaction, to thereby improperly retrieve the customer's Signature Phrase. By having the custom greeting 306, it will be difficult for the entity to duplicate the exact look of the
15 authorization form 300. The absence of the custom greeting 306 will notify the customer 14 that something is amiss.

There are additional ways to help prevent spoofing of the authorization form 300. For one, the authorization form can be provided by the authorization system 18 in GIF format, thereby making it difficult to modify its appearance. Additionally, the authorization form 300 may include
20 instructions (e.g., text or graphical) to direct the attention of the customer 14 to check the current URL of the browser on the computer 14a. The URL should be from the authorization system 18, and not some other entity (e.g., the merchant 16), thereby further notifying the customer 14 when something
25 is amiss.

The authorization form 300 also includes the merchant's name 308 and total amount 310 derived from the merchant provided data MID and AMT,

respectively. Furthermore, the authorization form 300 includes a date/time stamp 312 and a contract clause 314, thereby giving the authorization form the look and appearance of a conventional, paper charge slip. However, instead of executing a physical signature such as on a paper charge slip, the customer 14 executes the authorization form 300 by entering a Signature Phrase in the input 316. Since the Signature Phrase is a very confidential and personal item, it is very much like a physical signature. In another implementation, customer 14 executes the authorization form 300 by entering a PIN or other account code.

In one embodiment, the authorization form 300 can include a script 320 or other calculation module. The script 320 includes the hash function to convert the Signature Phrase or account code provided by the customer 14 into a hash value. Since the script 320 is part of the authorization form 300, it resides on the customer's computer 14a. As a result, the Signature Phrase or account code itself is never transmitted over the network 12, thereby reducing the likelihood of theft. In other embodiments, the actual Signature Phrase or account code may be securely transmitted over the network 12.

At step 260, the authorization process receives the Signature Phrase or account code, or hash thereof, as discussed above. In the case of an account code hash, the BUY button would have to include the actual account number in order to compute a correct hash to compare to an H3 record in the database 50. This would not be the case if the database 50 stored the actual account code. At step 262, the received data is compared with the appropriate entry of the database 50. According to the comparison, a RETURN code (such as from Table 5, above) is returned to the merchant 16.

Referring again to Fig. 5, at step 158, the returned RETURN code is analyzed. If the RETURN code indicates a successful authorization (e.g., value

3 of Table 5, above), execution proceeds to step 160 where the authorization is recorded and at step 162, the transaction is completed and fulfilled according to the merchant's (16) customary credit card authorization and fulfillment processes. If at step 158 the RETURN code does not indicate a successful authorization, execution proceeds to step 164 where further action may be employed.

Examples of further action may be dependent on the level of information provided to the merchant, such as may be indicated by the particular RETURN code. In the example of Table 5, RETURN codes 1, 2, and 4-11 indicate unsuccessful authorization.

If the RETURN code is 1, 2, or 7, the merchant 16 may wish to operate according to conventional fraud-detection techniques. For example, the merchant 16 can review internal lists of bad accounts or use external service providers to make a decision whether to complete and fulfill the transaction accordingly.

If the RETURN code is 5, the merchant 16 and/or the authorization system 18 can treat the transaction as fraudulent. The attempted transaction can be forwarded to the appropriate entities, such as the police or the account issuer, and/or the recipient(s) identified in the EMAILID (Table 1) can be informed.

If the RETURN code is 6, the customer can be informed of the restriction and a new transaction can be initiated. Furthermore, proper notification to a specific entity, such as to the recipient identified in the EMAILID, can be given.

If the RETURN code is 8-11, software or other correction may be required. In the interim, the merchant 16 may wish to operate according to conventional authorization and fraud-detection techniques.

Transaction Certificate

In some embodiments, the authorization system 18 may provide a transaction certificate to the merchant 16, the account issuer, and/or the customer 14. One goal of the certificate is to provide a self-validating record that authenticates and memorializes a specific execution of the authorization form 300 by the customer 14 for the transaction. Table 6 provides one embodiment of a certificate.

Item	Description
RETURN	Table 5, above
DATE/TIME	An exact time and date.
H1	Equation 1, above
H2	Equation 2, above
MID	Table 4, above
REF	Table 4, above
AMT	Table 4, above
H4	Hash of specific optional purchase information provided by merchant and acknowledged by customer
APPCODE	Approval code
OTHER2	Additional data
SEQ	Sequence number from the authorization system
ROOT	Root certificate of the authorization system
SIGNATURE	Digital signature from the authorization system

Table 6

Several of the items in the certificate of Table 6 are discussed elsewhere in the present disclosure. The RETURN code and DATE/TIME value are generated by the authorization process 250. For the utmost accuracy, an

atomic clock can be used to provide the DATE/TIME value. The values H1, H2, MID, AMT, and REF may be provided by the merchant 16 to the authorization system 18. The APPCODE may be a traditional approval code, such as provided by conventional credit card authorization or fraud detection systems, and may require external systems to participate in order to obtain this code.

The authorization system 18 hashes certain information included in Table 4 to generate the H4 value. In one embodiment, the H4 value is the hash of the TD item from Table 4. Including the H4 value in the transaction certificate uniquely associates the transaction certificate to the particular transaction description.

The SEQ value is a unique value given by the authorization system 18 for a specific certificate. For the sake of example, every certificate issued by the authorization system 18 may be numbered sequentially, e.g., 1, 2, 3, 4,

The ROOT value represents a root certificate of the authorization system 18. In one embodiment, the ROOT value includes a public encryption key for the authorization system 18, digitally signed by four separate private keys, whose corresponding public keys are known.

The SIGNATURE value is a digital signature provided by the authorization system 18. The authorization system 18 produces its digital signature by using a private key that corresponds to the ROOT public encryption key (discussed above) to digitally sign the transaction certificate. The process of digitally signing is described in greater detail in the presently incorporated U.S. Patent Application Ser. No. 09/340,853. Some or all of the items in the certificate are assembled and hashed for use in the digital signature. The digital signature thereby authenticates the transaction certificate and enables the merchant site system to confirm that the

information included in the transaction certificate originated at the site and has not been tampered with during transmission. Furthermore, the combination of the SIGNATURE and ROOT values makes the transaction certificate self-validating.

5 When the merchant 16 receives the transaction certificate, the merchant can perform a verification process to check the validity of the digital signature from the authorization system 18. Once the validity is confirmed, the merchant 16 can automatically process the transaction using conventional credit card authorization processing techniques, if applicable. If all tests pass,
10 a record can be formatted and stored per the merchant's specifications.

Conclusion

5 The authorization system enables customers to affirmatively assert "right-of-use" for a particular account or credit card by using, in one embodiment, a Signature Phrase that is linked to the account by an
15 affirmative activation process that uses the account issuer's specified account code for initial authentication. This, in turn, enables the merchant to complete and fulfill a transaction with a high degree of confidence that the authorizing customer is the account owner, or is at least authorized to use the account on the behalf of the owner. By establishing a Signature Phrase to
20 authorize transactions, customers and merchants alike are more likely to use e-commerce. In some embodiments, the Signature Phrase never leaves the customer's computer, and is therefore not subject to compromise. In some embodiments where the Signature Phrase is provided to the authentication system, the Signature Phrase can be modified through a transformation
25 function and then erased.

Alternatives such as additional Signature Phrases with restriction and notification requirements provide unique flexibility while maintaining a very secure transaction.

5 The authentication system does not require any unique customer side software for it to operate.

The authentication system provides a charge slip approach to e-commerce. The transaction certificate adds further integrity to the affirmative transaction authorization.

10 In case of a dispute between the customer and the merchant, the transaction certificate can affirmatively confirm what was authorized.

Since the transaction certificate is complete and self-validating, only the transaction certificate needs to be stored at the authorization system.

It is understood that modifications, changes and substitutions are intended in the foregoing disclosure and in some instances some features of the disclosure will be employed without corresponding use of other features. Furthermore, additional features may be employed without changing the operation of the present invention. For example, the authorization system may periodically check an account code and account number with a separate, commonly external authorization process. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the disclosure.